REMARKS

In the final Office Action, the Examiner rejected claims 1-3, 5-33, and 35-66 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1, 2, 5, 11, 14, 15, 18, 24, and 59 of Gavan et al. (U.S. Patent No. 7,117,191); and rejected claims 1-3, 5-33, and 35-66 under 35 U.S.C. § 103(a) as unpatentable over Bowman (U.S. Patent No. 5,627,886) in view of Phelps (U.S. Patent No. 5,602,906).

By this Amendment, Applicants propose amending claims 1, 28, and 61 to improve form. Applicants previously canceled claims 4 and 34, without prejudice or disclaimer of the subject matter thereof. No new matter is believed to have been added by way of the present Amendment. Applicants respectfully traverse the Examiner's double patenting rejection and the rejection under 35 U.S.C. § 103(a).[1] Claims 1-3, 5-33, and 35-66 would be pending upon entry of the present amendment.

OBVIOUSNESS-TYPE DOUBLE PATENTING REJECTION

On pages 2-4 of the final Office Action, the Examiner rejected claims 1-3, 5-33, and 35-66 under the judicially created doctrine of obviousness-type double patenting as allegedly unpatentable over claims 1, 2, 5, 11, 14, 15, 18, 24, and 59 of Gavan et al. Applicants respectfully traverse this rejection.

Without acquiescing in the Examiner's rejection, but simply to expedite prosecution, Applicants submit concurrently herewith a Terminal Disclaimer, disclaiming the terminal part of the statutory term of any patent granted on the instant application which would extend beyond

[1] As Applicants' remarks with respect to the Examiner's rejections are sufficient to overcome these rejections, Applicants' silence as to assertions by the Examiner in the Office Action or certain requirements that may be applicable to such rejections (e.g., whether a reference constitutes prior art, motivation to combine references) is not a concession by Applicants that such assertions are accurate or such requirements have been met, and Applicants

the expiration date of the full statutory term of Gavan et al. (U.S. Patent No. 7,117,191), as such term is defined in 35 U.S.C. §§ 154 and 173. The Terminal Disclaimer should render moot the obviousness-type double patenting rejection.

For at least the foregoing reasons, Applicants respectfully request the reconsideration and withdrawal of the judicially created doctrine of obviousness-type double patenting rejection of claims 1-3, 5-33, and 35-66 as allegedly unpatentable over claims 1, 2, 5, 11, 14, 15, 18, 24, and 59 of Gavan et al.

REJECTION UNDER 35 U.S.C. § 103(a) BASED ON BOWMAN AND PHELPS

On page 4 of the final Office Action, the Examiner rejected claims 1-3, 5-33, and 35-66 U.S.C. § 103(a) as allegedly unpatentable over Bowman in view of Phelps. Applicants initially note that on page 4 of the final Office Action, the Examiner listed claims 1-6 and 7-27 as being rejected under 35 U.S.C. § 103(a), but proceeded to reject claims 1-3, 5-33, and 35-66 on pages 4-24 of the final Office Action. Applicants respectfully traverse the Section 103(a) rejection with regard to the claims presented herein.

A. Claims 1-3 and 5-27

Amended independent claim 1, for example, is directed to a method for detecting fraud in one of a credit card or debit card system. The system generates network event records, where each network event record is generated in response to an event in the system. The method includes determining whether the system is a credit card system or a debit card system, performing at least one fraud detection test on the network event records based on the determination of whether the system is a credit card system or a debit card system, and

reserve the right to analyze and dispute such in the future.

generating a fraud alarm upon detection of suspected fraud by the at least one fraud detection test. The method also includes correlating fraud alarms based on common aspects of the fraud alarms, the correlated fraud alarms being consolidated into a fraud case, the fraud case being assigned a priority based on a severity of the suspected fraud, and responding to the fraud case with a fraud prevention action, the fraud prevention action being based on the priority assigned to the fraud case.

Bowman and Phelps, whether taken alone or in any reasonable combination, do not disclose or suggest the combination of features recited in claim 1. For example, Bowman does not disclose or suggest a method for detecting fraud in one of a credit card or debit card system, determining whether the system is a credit card system or a debit card system, or performing at least one fraud detection test on the network event records based on the determination of whether the system is a credit card system or a debit card system, as required by claim 1. Instead, Bowman discloses a fraud detection system for detecting and preventing fraudulent use of communications or credit card/business networks (col. 2, lines 45-47). Indeed, the words "debit card" do not appear in Bowman. Nowhere does Bowman disclose or remotely suggest a method for detecting fraud in one of a credit card or debit card system, determining whether the system is a credit card system or a debit card system, or performing at least one fraud detection test on the network event records based on the determination of whether the system is a credit card system or a debit card system, as required by claim 1.

The Examiner alleged that Bowman discloses performing at least one fraud detection test on the network event records based on the determination of whether the system is a credit card system or a debit card system, and cited Fig. 2, col. 2, lines 15-25 and 40-50, col. 3, line 60 – col. 4, line 5, and col. 17, lines 1-10 of Bowman for support (final Office Action, pages 4 and 5).

Applicants respectfully disagree with the Examiner's interpretation of Bowman.

Col. 5, line 19 – col. 6, line 32 of Bowman discusses Fig. 2 and discloses the architecture of the FMS. For example, at col. 5, line 60 – col. 6, line 5, Bowman states:

> An event record is a collection of data fields which describes an instance of network usage. Each event record contains all of the information about a call event that the system uses. FMS 10 preferably assigns each call event record an event type or category, based on the types of network services the record reflects. FMS 10 considers call events to be atomic (i.e., call events cannot span records). The following are some examples of event types: IDD calls, calling card calls, automatic collect calls, information services, other services, digital cellular calls, digital cellular forwarded calls, analog cellular calls, roaming calls. Other examples include event types resulting from the use of a video network, use of a data network or other use of a voice network.

In this section, Bowman discloses that a fraud management system (FMS) (and thus Fig. 2) is limited to detecting and preventing fraudulent use of communications or credit card/business networks. Nowhere in this section, or elsewhere, does Bowman disclose or suggest a method for detecting fraud in one of a credit card or debit card system, determining whether the system is a credit card system or a debit card system, or performing at least one fraud detection test on the network event records based on the determination of whether the system is a credit card system or a debit card system, as required by claim 1.

Col. 2, lines 15-25 of Bowman states:

> It is a further object of the present invention to provide a system and method for detecting network usage patterns indicative of fraud wherein such system and method support any combination of a plurality of disparate networks. Each of the networks are sources of respective network event records reflecting use of such network. Examples of such event records include call detail records from wireline, digital or analog cellular communications networks, or credit card usage and authorization records, roaming data (typically either real-time or via tape), video data, communications data, etc.

In this section, Bowman discloses a system and method for detecting fraud in wireline, digital or analog cellular communications networks, or credit card usage and authorization records, roaming data, video data, communications data, etc. Nowhere in this section, or elsewhere, does Bowman disclose or suggest a method for detecting fraud in one of a credit card or debit card system,

determining whether the system is a credit card system or a debit card system, or performing at least one fraud detection test on the network event records based on the determination of whether the system is a credit card system or a debit card system, as required by claim 1.

At col. 2, lines 40-50, Bowman states:

> The Fraud Management System (FMS) of the present invention effectively detects usage patterns indicative of many types of known fraud including: calling card related fraud, cellular phone fraud, subscription fraud, hacking, call selling, 900/800 fraud, and PBX or CPE fraud, among others. As a result, the FMS provides a means for detecting and ultimately preventing fraudulent use of communications or credit card/business networks. Monitoring network usage for fraudulent telecommunications network usage patterns according to the present invention takes place outside the switch and normally after the call event has completed.

In this section, Bowman discloses a fraud management system (FMS) for detecting and preventing fraudulent use of communications or credit card/business networks. Nowhere in this section, or elsewhere, does Bowman disclose or suggest a method for detecting fraud in one of a credit card or debit card system, determining whether the system is a credit card system or a debit card system, or performing at least one fraud detection test on the network event records based on the determination of whether the system is a credit card system or a debit card system, as required by claim 1. Indeed, Bowman cannot disclose this feature of claim 1 because the reference fails to disclose the words "debit card."

Col. 3, line 60 – col. 4, line 5 of Bowman states:

> DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS
>
> The system and method of the present invention effectively detects network usage patterns often indicative of many types of known fraud, including: calling card-related fraud, cellular phone fraud, subscription fraud, hacking, call selling, 900/800 fraud, PBX or CPE fraud, credit card fraud, etc. While not all unusual patterns of network usage indicate fraud, certain patterns are more likely than not to indicate the possibility of fraud and bear further investigation by a user or fraud analyst. It should be understood at this point that any user referred to herein may also be a system administrator or a fraud analyst, or both.

In this section, Bowman discloses a system and method for detecting fraud, including calling

card-related fraud, cellular phone fraud, subscription fraud, hacking, call selling, 900/800 fraud, PBX or CPE fraud, credit card fraud, etc. Nowhere in this section, or elsewhere, does Bowman disclose or suggest a method for detecting fraud in one of a credit card or debit card system, determining whether the system is a credit card system or a debit card system, or performing at least one fraud detection test on the network event records based on the determination of whether the system is a credit card system or a debit card system, as required by claim 1.

Col. 17, lines 1-10 of Bowman states:

> Frequently the specification of a call event type does not narrow the scope of analysis enough for meaningful conclusions. Additional data criteria, or screenings, are required to produce meaningful statistics. A screening is a test applied to one field in a call event. If the test is true, the screening is passed. For a measurement to produce a non-zero result all screenings attached to the measurement must be passed. FMS 10 supports a variety of types of screenings, including:
>
> List--The screening check performs a comparison against a list of discrete values using the contents of a field in the event.

In this section, Bowman discloses screening a call event. Nowhere in this section, or elsewhere, does Bowman disclose or suggest a method for detecting fraud in one of a credit card or debit card system, determining whether the system is a credit card system or a debit card system, or performing at least one fraud detection test on the network event records based on the determination of whether the system is a credit card system or a debit card system, as required by claim 1.

Likewise, Phelps does not disclose or suggest a method for detecting fraud in one of a credit card or debit card system, determining whether the system is a credit card system or a debit card system, or performing at least one fraud detection test on the network event records based on the determination of whether the system is a credit card system or a debit card system, as required by claim 1. In the final Office Action, the Examiner did not rely upon Phelps as

disclosing these features of claim 1. Furthermore, Phelps discloses a fraud detection system for use in a telecommunications system to detect unauthorized use of billing numbers (col. 1, lines 6-10). The words "debit card" do not appear in Phelps, and the words "credit card" only appear in Phelps in connection with a billing number of the telecommunications system (col. 2, line 49).

Further with regard to other features of claim 1, the Examiner admitted that "[w]hat Bowman does not explicitly teach is (3) correlating fraud alarms based on common aspects of the fraud alarms, the correlated fraud alarms being consolidated into a fraud case, the fraud case being assigned a priority based on a severity of the suspected fraud; and (4) responding to the fraud case with a fraud prevention action, the fraud prevention action being based on the priority assigned to the fraud case." (final Office Action, page 5). However, the Examiner alleged that Phelps teaches these features of claim 1 (final Office Action, page 5).

Since Phelps is limited to a telecommunications fraud detection system, Phelps cannot disclose the other features recited in claim 1, such as correlating fraud alarms based on common aspects of the fraud alarms, the correlated fraud alarms being consolidated into a fraud case, the fraud case being assigned a priority based on a severity of the suspected fraud, and responding to the fraud case with a fraud prevention action, the fraud prevention action being based on the priority assigned to the fraud case.

The Examiner alleged that Phelps discloses correlating fraud alarms based on common aspects of the fraud alarms, the correlated fraud alarms being consolidated into a fraud case, the fraud case being assigned a priority based on a severity of the suspected fraud, and cited col. 2, lines 30-40, col. 2, line 63 – col. 3, line 5, and col. 4, lines 40-50 of Phelps for support (final Office Action, page 5). Applicants respectfully disagree with the Examiner's interpretation of Phelps.

Col. 2, lines 30-40 of Phelps states:

> Apparatus 10 receives call placement information and customer information from network 12. This information is used to update the history information stored in apparatus 10. Apparatus 10 generates an indication of unauthorized use of a billing number by applying the call placement and history information to a set of expert system rules. The indication is a case that is generated from an alert and assigned a priority. The case is resolved by a set of expert system rules or a researcher, and network 12 acts on the resolution.

In this section, Phelps discloses that the detection system applies the call placement and history information to set of expert system rules to determine an indication of unauthorized use. Nowhere in this section, or elsewhere, does Phelps disclose or suggest correlating fraud alarms based on common aspects of the fraud alarms, the correlated fraud alarms being consolidated into a fraud case, the fraud case being assigned a priority based on a severity of the suspected fraud, in a method for detecting fraud in one of a credit card or debit card system, as required by claim 1.

Col. 2, line 63 – col. 3, line 5 of Phelps states:

> SCPMS 44 processes call attempt information and produces alerts that are provided to SCPMS gateway 18. These alerts are generated for LEC and IXC calling cards only when the number of attempts to use a calling card exceeds a predetermined threshold. The threshold is dependant in part on the type of product and the geographic dispersion of the call origination points. SCPMS gateway 18 analyzes the alerts based on a set of expert system rules for the detection of fraudulent call activity, and generates alerts based on the SCPMS alerts to send to central computer 20 for further analysis.

In this section, Phelps discloses that the detection system generates alerts when attempts to use a calling card exceed a predetermined threshold. Nowhere in this section, or elsewhere, does Phelps disclose or suggest correlating fraud alarms based on common aspects of the fraud alarms, the correlated fraud alarms being consolidated into a fraud case, the fraud case being assigned a priority based on a severity of the suspected fraud, in a method for detecting fraud in one of a credit card or debit card system, as required by claim 1.

Col. 4, lines 40-50 of Phelps states:

> The expert system rules are configured empirically on the basis of actual cases of unauthorized billing number usages. With this approach, the rules can be continuously updated and refined to reflect learning experiences concerning newly detected cases of toll fraud, and customized for each type of billing number. Thus, those skilled in the art will appreciate that the rules are not fixed, but are continuously evolving in order to adapt to the most current conditions.

In this section, Phelps discloses that the detection system uses expert system rules that may be updated to reflect learning experiences concerning newly detected toll fraud. Nowhere in this section, or elsewhere, does Phelps disclose or suggest correlating fraud alarms based on common aspects of the fraud alarms, the correlated fraud alarms being consolidated into a fraud case, the fraud case being assigned a priority based on a severity of the suspected fraud, in a method for detecting fraud in one of a credit card or debit card system, as required by claim 1.

The Examiner alleged that Phelps discloses responding to the fraud case with a fraud prevention action, the fraud prevention action being based on the priority assigned to the fraud case, and cited col. 2, lines 30-40, and col. 2, line 63 – col. 3, line 5 of Phelps for support (final Office Action, page 5). Applicants respectfully disagree with the Examiner's interpretation of Phelps.

Col. 2, lines 30-40 of Phelps is reproduced above and discloses that the detection system applies the call placement and history information to set of expert system rules to determine an indication of unauthorized use. Nowhere in this section, or elsewhere, does Phelps disclose or suggest responding to the fraud case with a fraud prevention action, the fraud prevention action being based on the priority assigned to the fraud case, in a method for detecting fraud in one of a credit card or debit card system, as required by claim 1.

Col. 2, line 63 – col. 3, line 5 of Phelps is reproduced above and discloses that the detection system generates alerts when attempts to use a calling card exceed a predetermined

threshold. Nowhere in this section, or elsewhere, does Phelps disclose or suggest responding to the fraud case with a fraud prevention action, the fraud prevention action being based on the priority assigned to the fraud case, in a method for detecting fraud in one of a credit card or debit card system, as required by claim 1.

Finally, Applicants submit that the Examiner failed to provide a proper motivation to combine Bowman and Phelps with respect to claim 1. On pages 5 and 6 of the final Office Action, the Examiner alleged:

> Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Bowman and incorporate the method of (3) correlating fraud alarms based on common aspects of the fraud alarms, the correlated fraud alarms being consolidated into a fraud case, the fraud case being assigned a priority based on a severity of the suspected fraud; and (4) responding to the fraud case with a fraud prevention action, the fraud prevention action being based on the priority assigned to the fraud case in view of the teachings of Phelps in order to ensure that cases with high priority or severity level are given adequate attention and proper resolution.

Applicants submit that this allegation is merely a conclusory statement regarding an alleged benefit of the combination. Such conclusory motivation statements have consistently been held by courts to be insufficient for establishing a *prima facie* case of obviousness. In this respect, Applicants rely upon In re Deuel, 51 F.3d 1552, 34 U.S.P.Q.2d 1210 (Fed. Cir. 1995), where it was held that generalizations do not establish the realistic motivation to modify a specific reference in a specific manner to arrive at a specifically claimed invention. Applicants submit that the final Office Action's purported motivation to combine the cited references is merely conclusory and based on impermissible hindsight.

Applicants further note that at page 9 of the final Office Action, the Examiner improperly failed to provide any motivation to combine Bowman with Phelps to arrive at the combination of features recited in claim 18.

For at least these reasons, Applicants submit that claim 1 is patentable over Bowman and

Phelps, whether taken alone or in any reasonable combination. Claims 2, 3, and 5-27 depend from claim 1 and are, therefore, patentable over Bowman and Phelps, whether taken alone or in any reasonable combination, for at least the reasons given with regard to claim 1.[2]

B. Claims 28-33 and 35-66

Amended independent claim 28 is directed to a system for monitoring one or more of a plurality of credit card or debit card networks, each network being configured to generate network event records, each network event record being generated in response to an event occurring in the network. The system comprises a fraud detection system including a core computing infrastructure and a domain specific infrastructure. The domain specific infrastructure is dynamically reconfigurable in accordance with the domain specific implementation of the network being monitored. The core computing infrastructure is non-domain specific. The fraud detection system is configured to determine whether the network is a credit card network or a debit card network, to analyze each network event record, and to perform a fraud prevention action in response to detecting an occurrence of fraud in the network event record and based on the determination of whether the network is a credit card network or a debit card network.

Bowman and Phelps, whether taken alone or in any reasonable combination, do not disclose or suggest the combination of features recited in claim 28. For example, Bowman does not disclose or suggest a fraud detection system configured to determine whether the network is a credit card network or a debit card network, to analyze each network event record, and to

[2] As Applicants' remarks with respect to the base independent claims are sufficient to overcome the Examiner's rejections of all claims dependent therefrom, Applicants' silence as to the Examiner's assertions with respect to dependent claims is not a concession by Applicants to the Examiner's assertions as to these claims, and Applicants reserve the right to analyze and dispute such assertions in the future.

perform a fraud prevention action in response to detecting an occurrence of fraud in the network event record and based on the determination of whether the network is a credit card network or a debit card network, as required by claim 28. Instead, Bowman discloses a fraud detection system for detecting and preventing fraudulent use of communications or credit card/business networks (col. 2, lines 45-47). Indeed, the words "debit card" do not appear in Bowman. Nowhere does Bowman disclose or remotely suggest a fraud detection system configured to determine whether the network is a credit card network or a debit card network, to analyze each network event record, and to perform a fraud prevention action in response to detecting an occurrence of fraud in the network event record and based on the determination of whether the network is a credit card network or a debit card network, as required by claim 28.

The Examiner alleged that Bowman teaches the fraud detection system recited in claim 28, and cited Fig. 2, col. 2, lines 40-67, and col. 4, lines 5-40 of Bowman for support (final Office Action, pages 13 and 14). Applicants respectfully disagree with the Examiner's interpretation of Bowman.

Col. 5, line 19 – col. 6, line 32 of Bowman discusses Fig. 2 and discloses the architecture of the fraud management system (FMS), and that the FMS (and thus Fig. 2) is limited to detecting and preventing fraudulent use of communications or credit card/business networks. Nowhere in this section, or elsewhere, does Bowman disclose or suggest a fraud detection system configured to determine whether the network is a credit card network or a debit card network, to analyze each network event record, and to perform a fraud prevention action in response to detecting an occurrence of fraud in the network event record and based on the determination of whether the network is a credit card network or a debit card network, as required by claim 28.

Col. 2, lines 40-67 of Bowman states:

> The Fraud Management System (FMS) of the present invention effectively detects usage patterns indicative of many types of known fraud including: calling card related fraud, cellular phone fraud, subscription fraud, hacking, call selling, 900/800 fraud, and PBX or CPE fraud, among others. As a result, the FMS provides a means for detecting and ultimately preventing fraudulent use of communications or credit card/business networks. Monitoring network usage for fraudulent telecommunications network usage patterns according to the present invention takes place outside the switch and normally after the call event has completed.
>
> The system monitors network usage on an event-by-event basis, accepting event record detail information from multiple network sources. As fraud is dynamic, exploiting new technologies and services nearly as quickly as they are deployed, the system also possesses a high degree of configurability. Fraud system administrators are able to create new detection mechanisms without the need to write new programs. Finally, the system and method of the present invention supports an analysis of trends in network usage, so that "early warnings" of new types of fraud are available.
>
> The system and method of the present invention assists in detecting fraudulent use of a communications network by monitoring the network to detect usage patterns typically indicative of fraud. The present system is not limited to detecting the types of fraud known to exist today. It is a general-purpose system that can be configured to detect many different sorts of usage patterns.

In this section, Bowman discloses a fraud management system (FMS) for detecting and preventing fraudulent use of communications or credit card/business networks. Nowhere in this section, or elsewhere, does Bowman disclose or suggest a fraud detection system configured to determine whether the network is a credit card network or a debit card network, to analyze each network event record, and to perform a fraud prevention action in response to detecting an occurrence of fraud in the network event record and based on the determination of whether the network is a credit card network or a debit card network, as required by claim 28.

Col. 4, lines 5-40 of Bowman states:

> It should be understood at this point that any user referred to herein may also be a system administrator or a fraud analyst, or both.
>
> According to a preferred embodiment of the present invention, FMS has a client-server architecture where a server will accept and respond to requests from multiple clients. Such architecture enables FMS to be easily distributed. FIG. 1 is a schematic diagram illustrating the distributed hardware architecture of the fraud monitoring system 10

according to the present invention.

Architecture 10 comprises FMS server 40 and one or more client workstations 20,25,30. FMS server 40 receives event records in batch or real-time from remote, local service control point(s) (SCPs) 50, switch(es) 60, pricing system(s) 75, and/or other computer(s) 65 via data collectors 100. Pricing System 75 provides priced event records such as priced call detail records to FMS server 40 for analysis. Switch(es) 60 may be any type of switch which reflects utilization of the network to which it is attached.

Depending upon the results of the analysis performed on the event records by the fraud detection engine (seen on FIG. 2) residing within FMS server 40 according to predefined conditions (explained later), FMS server 40 will send alarms to, and will respond to queries from, select users at client workstations 20,25,30. It should be understood that one or more workstations 20 may be employed to implement FMS 10. Client workstations 20,25,30 may be networked to FMS server 40 via a local area network (LAN) line or may be more remote. FMS 10 is preferably implemented with an Ethernet backbone.

FMS server 40 also interacts with Network Management System 70 and printer 80. Network Management System 70 is typically responsible for monitoring and controlling the elements and communication links which comprise a network.

In this section, Bowman discloses the hardware architecture for a fraud management system (FMS) for detecting and preventing fraudulent use of communications or credit card/business networks. Nowhere in this section, or elsewhere, does Bowman disclose or suggest a fraud detection system configured to determine whether the network is a credit card network or a debit card network, to analyze each network event record, and to perform a fraud prevention action in response to detecting an occurrence of fraud in the network event record and based on the determination of whether the network is a credit card network or a debit card network, as required by claim 28.

Likewise, Phelps does not disclose or suggest a fraud detection system configured to determine whether the network is a credit card network or a debit card network, to analyze each network event record, and to perform a fraud prevention action in response to detecting an occurrence of fraud in the network event record and based on the determination of whether the network is a credit card network or a debit card network, as required by claim 28. In the final

Office Action, the Examiner did not rely upon Phelps as disclosing these features of claim 28. Furthermore, Phelps cannot possibly disclose these features because the words "debit card" do not appear in Phelps, and the words "credit card" only appear in Phelps in connection with a billing number of the telecommunications system (col. 2, line 49).

For at least these reasons, Applicants submit that claim 28 is patentable over Bowman and Phelps, whether taken alone or in any reasonable combination. Claims 29-33 and 35-66 depend from claim 28 and are, therefore, patentable over Bowman and Phelps, whether taken alone or in any reasonable combination, for at least the reasons given with regard to claim 28.[3]

In light of the above, Applicants respectfully request the reconsideration and withdrawal of the 35 U.S.C. § 103(a) rejection of claims 1-3, 5-33, and 35-66 as allegedly unpatentable over Bowman and Phelps.

CONCLUSION

In view of the foregoing amendments and remarks, Applicants respectfully request the Examiner's reconsideration of the application and the timely allowance of pending claims 1-3, 5-33, and 35-66. Applicants respectfully request entry of the present amendment because the present amendment does not raise new issues or require a further search of the art since the features were previously examined by the Examiner. Moreover, Applicants submit that the present amendment places the application in better condition for appeal should the Examiner contest the patentability of the pending claims.

If the Examiner does not believe that all pending claims are now in condition for

[3] As Applicants' remarks with respect to the base independent claims are sufficient to overcome the Examiner's rejections of all claims dependent therefrom, Applicants' silence as to the Examiner's assertions with respect to dependent claims is not a concession by Applicants to the Examiner's assertions as to these claims, and Applicants reserve the right to analyze and dispute such assertions in the future.

allowance, the Examiner is urged to contact the undersigned to expedite prosecution of this application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-1070 and please credit any excess fees to such deposit account.

Respectfully submitted,

HARRITY SNYDER, L.L.P.

By: /James M. Olsen/
James M. Olsen
Reg. No. 40,408

Date: February 7, 2006
11350 Random Hills Road
Suite 600
Fairfax, Virginia 22030
Phone: (302) 478-4548
Fax: (571) 432-0808
CUSTOMER NUMBER: 25537